CLAIMS

1. Resource allocation method for a security module of an apparatus connected to a network, this network being administrated by an operator (OP), said resources (RSC) being used by application suppliers (FO), this method comprising the following steps:

- generating a pair of asymmetric keys and storage of the private key in the security module (US-SM), the public key (KPuUS) being stored by an authority (IS),
- introducing at least one public key of the authority (KPuIS) in the security module (US-SM),
- the operator (OP) receiving a request from a supplier (FO) and transmission of this request to the authority (IS), this request comprising at least the supplier's public key (KPuFO),
- transmission by the operator (OP) of a resource reservation instruction (RSC) to the security module (US-SM) together with the supplier's public key (KPuFO),
- transmission by the operator (OP) of the public key (KPuUS) of the security module to the supplier (FO),
- establishment of a secure communication channel between the supplier (FO) and the security module (US-SM),
- loading of an application in the security module (US-SM) by the supplier (FO).

2. Resource allocation method according to claim 1, characterized in that the pair of asymmetric keys is generated by the security module, the public key then being transmitted to the authority.

3. Resource allocation method according to claim 1, characterized in that the initialization parameters of a session key (M, b) pertaining to the operator are stored in the security modules during the initialization.

4. Resource allocation method according to claims 1 to 3, characterized in that the supplier transmits the initialization parameters of a session key (M, b) to the operator, these parameters being transmitted to the security module during the reservation of a resource.

5. Resource allocation method according to claims 1 to 4, characterized in that the establishment of a secure communication between the supplier and the security module is based on the use of the supplier's public key by the security module and the use of the security module's public key by the supplier.

6. Resource allocation method according to claim 3, characterized in that the establishment of a secure communication between the operator and the security module is based on the generation of a session key using the initialization parameters (M, b) of the operator.

7. Resource allocation method according to claim 4, characterized in that the establishment of a secure communication between the supplier and the security module is based on the generation of a session key using the initialization parameters (M, b) of the supplier.

8. Resource allocation method according to one of the previous claims, characterized in that the authority (IS) and the operator (OP) form the same entity.

9. Resource allocation method according to one of the previous claims, characterized in that the resource reservation instruction (RES) includes the sending of a domain key (DK), which is specific to an application and common to all the security modules having this application, this key being used for the establishment of a secure communication between the supplier FO and the security module.